u-헬스케어 환경에서 환자의 무결성을 보장하는 RFID 보안 프로토콜

이봉근* · 정윤수** · 이상호***

Privacy Model based on RBAC for U-Healthcare Service Environment

Bong-Keun Rhee* · Yoon-Su Jeong** · Sang-Ho Lee***

요 약

최근 유비쿼터스 컴퓨팅 기술 분야 중 사용자의 정보 속성이 매우 민감한 u-헬스케어가 의료분야에서 각광을 받고 있다. u-헬스케어는 개인 건강/의료 정보를 포함한 극히 개인적인 정보를 다루고 있기 때문에 보안 및 프라이버시 측면에서 다양한 취약점 존재 및 위협에 노출되어 있다. 본 논문에서는 환자가 소유하고 있는 휴대장치(PDAs나 휴대용 컴퓨터)를 제 3자가 불법적으로 악용하여 환자의 정보를 훼손하는 것을 예방하기 위한 RFID 기반의 환자 정보 보호 프로토콜을 제안한다. 제안 프로토콜은 사전에 관리 서버에 등록된 병원(의사, 간호사, 약국 등)의 권한 정보에 따라 환자의 개인정보에 접근할 수 있도록 병원(의사, 간호사, 약국 등)의 권한을 계층적으로 분리하여 병원이 최소한의 업무를 수행하도록 한다. 특히, 게이트웨이 역할하는 관리 서버는 접근 허가가 승인된 환자 정보 이외에 허가받지 않은 정보에 대해서 제 3자가 쉽게 접근하지 못하도록 주기적으로 접근 허용 키를 생성하여 환자의 인증 및 관리의 효율성을 향상시키고 있다.

ABSTRACT

Nowadays u-healthcare which is very sensitive to the character of user's information among other ubiquitous computing field is popular in medical field. u-healthcare deals extremely personal information including personal health/medical information so it is exposed to various weaknees and threats in the part of security and privacy. In this paper, RFID based patient's information protecting protocol that prevents to damage the information using his or her mobile unit illegally by others is proposed. The protocol separates the authority of hospital(doctor, nurse, pharmacy) to access to patient's information by level of access authority of hospital which is registered to management server and makes the hospital do the minimum task. Specially, the management server which plays the role of gateway makes access permission key periodically not to be accessed by others about unauthorized information except authorized information and improves patient's certification and management.

키워드

u-헬스케어, RFID, 프로토콜, 무결성

Key word

u-Healthcare, RFID, Protocol, Confidence

* 정회원 : 부산경상대학 소방안전계열 (제1저자, rbk@bsks.ac.kr)
** 정회원 : 목원대학교 정보통신공학과 교수 (bukmunro@gmail.com)
*** 정회원 : 충북대학교 소프트웨어학과 교수 (교신저자, shlee@chungbuk.ac.kr)

접수일자 : 2011. 06. 22
심사완료일자 : 2011. 08. 06

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.3.605

Ⅰ. 서 론

고령화 사회 진입, 만성질환 증가, 건강에 대한 관심 증대로 인하여 언제 어디서나 건강관리 서비스를 받을 수 있는 u-헬스케어 서비스가 최근에 주목받고 있다. u-헬스케어는 유비쿼터스 정보통신기술을 보건의료산업에 접목함으로써 사용자가 언제 어디서나 휴대용 도구를 이용하여 건강상태를 확인하고 관리할 수 있는 보건의료 서비스를 의미한다[1,2].

정보통신기술, 바이오 센서 및 스마트 의료기기의 발달은 u-헬스케어 관련 기술의 개발을 가속화하고 있으며, 스마트 케어, 글로벌 u-헬스케어 센터 등 정부 차원의 u-헬스케어 관련 사업, 지방 자치단체들이 시범운영하는 만성질환 관리 u-헬스케어 서비스, 보건복지부의 원격진료를 일부 허용하는 의료법 개정안 마련 등 관련 부처의 제도적 기반 구축 노력은 u-헬스케어 시대의 도래를 예고하고 있다[3,4].

u-헬스케어 서비스의 첨단 의료 환경에서 의료 사고를 줄이기 위해서 최근에는 환자의 의료 프로필을 이용하여 환자를 쉽게 식별할 수 있도록 RFID 기술을 많이 적용하고 있다[5,6]. u-헬스케어 서비스에서는 환자의 개인정보를 PDAs(Personal Digital Assistants)나 휴대용 컴퓨터를 사용하여 환자 개인정보를 언제, 어디서든 최신의 갱신된 개인정보에 접근할 수 있도록 도와주지만 제3자의 악의적인 행위로 인하여 환자의 개인정보가 노출되고 있다[7,8].

u-헬스케어 서비스의 활성화는 의료 서비스의 질을 높이며 보건의료 취약계층에게 의료 혜택을 제공할 것으로 예상되지만 의료 사고 발생 시의 법적 책임 소재가 불명확, 건강보험수가 불안정, 개인정보보호 문제 미해결, 의료정보표준 미비 등의 제도적 문제 발생 가능성이 있어 개선이 필요하다. 또한, 다양한 의료 센서 및 의료기기의 이용과 건강정보에 대한 연계 및 공유로 인해 개인의 생체 정보, 헬스케어 서비스 정보, 행동 특성, 생활정보 등 개인에 대한 방대한 정보 수집이 가능해질 수 있기 때문에 개인정보보호에 대한 연구가 필요하다[9,10].

이 논문에서는 PDAs나 휴대용 컴퓨터를 사용하는 환자의 개인정보를 제3자가 획득할 수 없도록 관리자의 보안 기능 및 관리를 강화할 수 있는 RFID 기반의 보안 프로토콜을 제안한다. 제안 프로토콜은 사용자의 권한확인 및 기록접근제어 등을 통하여 환자, 병원, 약국의 권한을 분리하여 최소한의 업무를 수행할 수 있도록 관리서버가 게이트웨이 역할을 수행한다. 또한, 관리 서버에 등록된 정보 이외에 허가받지 않은 제 3자가 쉽게 환자의 민감한 의료정보 및 개인정보에 접근하지 못하도록 환자와 관리 서버간 주기적인 공유키 생성을 통해 환자의 인증 및 관리의 효율성을 향상시킨다.

이 논문의 구성은 다음과 같다. 2장에서는 u-헬스케어 서비스의 개념과 보안 문제에 대해서 알아본다. 3장에서는 환자 정보의 무결성을 보장하는 RFID 기반의 사용자 인증 프로로토콜을 제안한다. 4장에서는 보안 공격에 따른 제안 프로토콜의 보안 평가를 분석하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1. u-헬스케어 서비스

u-헬스케어 서비스는 인체의 건강 관련 정보를 언제, 어디서나 수집, 처리, 전달, 관리 할 수 있게 함으로써 환자의 질병 증상을 완화, 치료하는 것에서 일반인의 건강을 증진하고 질병을 예방하고 관리하는 새로운 형태의 건강관리 및 의료서비스를 의미한다[1,8].

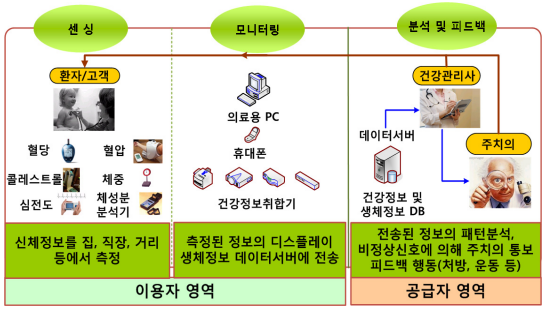

그림 1. u-헬스케어 서비스 개념도
Fig. 1 u-Healthcre Service Design

[그림 1]은 u-헬스케어 서비스에 대한 개념도로써 u-헬스케어 서비스를 구성하는 항목은 센싱, 모니터링, 분석 및 피드백으로 구성된다. 센싱은 인체에서 발생하는 물리적·화학적인 현상의 변화를 감지하여 처리 가능한 전기적 신호로 변환하는 곳이며, 모니터링은 측정된 생체정보를 의미 있는 생체신호 성분만을 선택하기 위

한 필터링 처리와 의미 있는 정보로 만들기 위한 분석과정, 그리고 이를 시각화하기 위한 과정으로 구성된다. 분석은 단순히 현재의 상태를 모니터링 할 뿐만 아니라, 장시간에 걸쳐 측정된 데이터로부터 건강상태, 생활패턴 등을 나타내는 새로운 건강자료를 분석하는 과정이다. 피드백은 장시간에 걸쳐 파악된 건강 기지선이나 생활의 변화를 사용자의 행동변화, 경고 등으로 사용자에게 제공하는 과정이다.

2.2. u-헬스케어 보안 문제

의료 서비스 기술이 발달함에 따라 u-헬스케어의 의료정보 보안에 대한 요구가 급증하고 있으며, PKI 또는 데이터 암호화 등을 중심으로 보안 기술들을 제품에 적용하고 있다[2].

u-헬스케어 환경에서 데이터 보호 및 프라이버시 보호 문제와 관련된 다양한 보안 취약점과 위협 요소들은 유·무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점과 유사하지만, 기존 유·무선 네트워크 기반 서비스와는 다른 보안 요구사항이 존재한다[9,10].

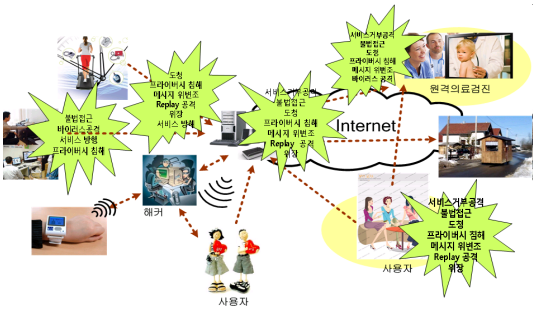

그림 2. u-헬스케어 환경의 보안 위협
Fig. 2 Security Threat of u-Healthcre Environment

[그림 2]에서 u-헬스케어 서비스의 주요 보안 위협은 화상시스템 해킹, 불법적인 접근, 도청/위변조, 의료장비 해킹, 웹 해킹, 개인 및 의료정보 DB 해킹, 의료망 침투 등이 있다[8].

의료 서비스 정보는 환자가 이동함에 따라 중복된 검사와 의료 조치를 선택적으로 다른 의료 기관(병·의원 또는 보건소 등)에 위임할 때 개인 정보는 의료 서비스 목적에 맞게 최소한으로 공유할 수 있다. 그러나 현재 의료 정보 보안 정책 및 기술로는 그 범위를 명확하게 파악하거나 결정할 수 없는 문제가 있다. 또한 불법적인 의료 정보 열람과 이용을 막고 그 책임 소재를 판단하기 위한 보안 감사 체계가 보완되어야 한다. 대부분의 병원에서는 요청자의 단순 서비스 요청에 관한 로그만 남길 뿐, 데이터 습득 이후 활용, 폐기 등에 관한 의무사항 준수에 관련한 감사 체계가 부재하여 내부자에 의한 정보 유출의 위험성이 높다. u-헬스케어 환경에서는 ID/PW나 공인 인증서 기반뿐만 아니라 다양한 생체 식별 정보가 사용자 인증 방식으로 활용되지만 생체 정보는 그 정보의 변경이 쉽지 않아 생체정보의 노출로 더 이상 사용이 불가능한 경우의 문제점이 발생할 수 있다.

Ⅲ. 환자의 개인정보 무결성 보장을 위한 계층적 키 관리 프로토콜

u-헬스케어 환경에서는 환자의 개인정보를 PDAs나 휴대용 컴퓨터를 사용하여 환자 개인정보를 언제, 어디서든 최신의 갱신된 개인정보에 접근할 수 있도록 도와주지만 제3자에 의한 환자의 개인정보 노출 위험이 있다. 이 절에서는 u-헬스케어 서비스를 제공하는 병원의 관리자가 보유하고 있는 공유키를 악의적인 공격자가 획득할 수 없도록 환자의 개인 정보와 관리 서버의 비밀 키를 주기적으로 XOR하여 환자의 개인정보를 안전하게 접근할 수 있는 보안 관리 프로토콜을 제안한다.

3.1. 보안 관리 프로토콜 제안 모델

환자의 프라이버시 위협이 증가되는 u-헬스케어 환경에서 병원이나 약국에서 환자의 기록을 이용할 경우에 제안 모델에서는 [그림 3]처럼 접근 권한에 따라 진찰 및 치료 내역을 이용할 수 있도록 사용자의 ID를 서버에서 통합 관리한다.

제안 프로토콜에서는 사용자의 권한확인 및 기록접근제어 등을 통하여 환자, 병원, 약국의 권한을 계층적으로 분리하여 최소한의 업무를 줌으로써 허가받지 않는 제 3자가 쉽게 환자의 민감한 의료정보 및 개인정보에 접근하지 못하도록 함으로써 환자 인증 및 관리 효율성을 향상시킨다.

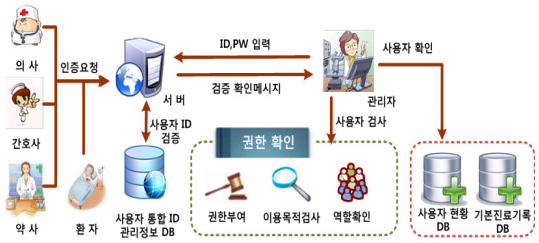

그림 3. 사용자 프라이버시 보장을 위한 제안 모델
Fig. 3 Proposed Model for User Privacy Assurance

제안 프로토콜을 구성하는 구성요소는 [그림 4]처럼 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서나 기기, 센서 간 통신 및 데이터 송·수신을 위한 유·무선 네트워크, 생체데이터 분석과 건강 피드백을 담당하는 의료 정보 서버, 그리고 생성된 의료 정보를 소비하는 다양한 정보 소비자 집단, 즉 환자나 의료진 및 관련 응용 서비스, 사용자 정보를 저장 및 관리하는 데이터베이스 등으로 구성된다.

[그림 4]에서 제안 프로토콜의 가정은 다음과 같다.

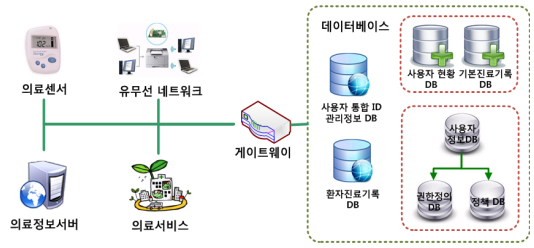

그림 4. 제안 모델의 구성요소
Fig. 4 Component of proposed model

① 센서나 기기

센서나 기기가 신뢰성이 있다거나 악의적으로 사용할 수 있다는 가정을 만들지 않는다. 각 센서나 기기는 u-헬스케어 서비스 전에 pair-wise 키를 부여 받으며, 네트워크가 동작되는 동안 센서나 기기만이 사용자의 센서 판독 정보를 수집 한다.

② 의료 정보 서버

u-헬스케어상에 존재하는 모든 기기는 서버와 직접 통신 가능하며 게이트웨이간 통신은 홉간 통신을 한다고 가정한다 게이트웨이의 주요 임무는 기기로부터 전달받은 데이터를 수집 및 전송하는 역할을 한다.

③ 데이터베이스

데이터베이스는 u-헬스케어 서비스에서 생성된 의료정보(환자나 의료진 및 관련 응용 서비스, 사용자 정보)를 저장 및 관리하는 역할을 수행한다.

표 1. 용어정리
Table. 1 Terminology

용어	개념
SID	보안 인식자
ID_x	x의 인식자
k_x	x의 비밀키
C_x	환자 x의 비밀키 값
H_x	x의 정보(비밀키, 보안인식자, 타임스탬프 등)를 해쉬한 결과를 대체한 값
T	타임스탬프
$\oplus$	xor 연산
$\|\|$	연접
$E(x, Data)$	키 x를 사용하여 $Data$를 암호화
$D(x, Data)$	키 x를 사용하여 $Data$를 복호화

3.2. 보안 관리 프로토콜 용어 정의

[표 1]은 제안된 프로토콜에서 사용되는 용어를 정의하고 있다.

3.3. 계층적 보안 관리 프로토콜

u-헬스케어 서비스의 계층적 보안 관리의 설정 단계에서는 u-헬스케어 서비스를 제공받는 사용자들에게 접근 제어를 수행하기 위한 키 분배와 접근 권한에 따라 사용자 그룹을 계층적으로 분류하는 과정으로 구성된다. u-헬스케어 서비스를 사용하는 모든 사용자들은 [그림 5]처럼 계층적으로 관리서버가 관리할 수 있도록 top-down 형태의 구조를 가지게 된다.

[그림 5]에서 중간 계층의 관리서버는 u-헬스케어 서비스의 안전성을 보장하기 위해서 상위 계층(병원, 의사, 간호사, 약사)과 하위 계층(환자)사이에서 중재자 역할을 하며, u-헬스케어 서비스를 제공받는 환자는 키와 ID를 오프라인으로 관리 서버에 등록한다. 일단 계층적 관계가 형성되면 관리자와 환자는 상호간의 안전한 통신에 이용되는 키를 생성하기 위해서 중간 계층 역할을 담당하는 관리자가 환자들의 개인정보와 XOR한다.

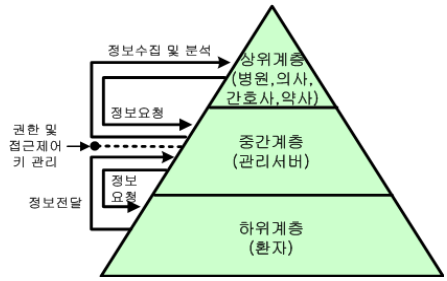

그림 5. 계층적 보안 관리 구조
Fig. 5 Hierachical Security Management Design

관리서버의 데이터베이스에 저장되는 정보는 사용자 정보의 이중 사용을 예방하기 위해서 사용자 인증 전에 이중 사용 정보를 관리서버가 체크한다. 이 때, 관리서버는 사용자의 개인정보가 이중으로 사용되는 것을 체크하기 위해서 (그림 6)과 같은 필드를 사용자에 부착된 장치로부터 전달받아 관리서버의 데이터베이스에 저장되어 있는 정보와 비교 후 정보가 일치할 경우 통신을 지속하고 일치하지 않으면 통신을 중지하도록 한다.

SID	ID_x	k_x	T	C_p	H_x	$CheckInfo$

그림 6. 관리서버의 데이터베이스에 저장된 레코드 정보
Fig. 6 Record Information saved within Database of Management Server

[그림 6]은 관리서버의 데이터베이스에 저장되는 각 필드의 세부적인 정보는 다음과 같다.

- SID : 환자의 보안인식자
- ID_x : 환자 x 정보의 임시 인식자
- k_x : x의 비밀키
- T : 타임스탬프
- C_p : 환자의 비밀키 값
- H_x : x의 정보(비밀키, 보안인식자, 타임스탬프 등)를 해쉬한 결과를 대체한 값
- $CheckInfo$: 사용자의 권한정보

3.3.1. 설정단계

설정 단계에서는 u-헬스케어 서비스를 사용하는 사용자들이 자신들의 의료 정보를 식별할 수 있는 비밀키를 등록하는 단계이다. u-헬스케어 서비스를 사용하는 모든 환자들은 자신의 의료정보를 식별할 수 있도록 RFID 태그가 부착된 전자팔찌나 스마트 밴드 형태의 장치를 착용하고 있음을 가정하고, 의사, 간호사, 직원 등도 환자의 개인정보에 접근하기 위해서 안전한 채널을 통해 자신의 정보를 등록해야 한다.

설정단계의 세부적인 동작 과정은 3단계로 동작되며 환자들에게 부착된 장치는 관리서버의 인증을 위해 키 설정을 한번만 수행된다.

■ 1단계 :

각 환자는 사전에 관리 서버로부터 부여받은 보안 인식자 SID를 이용하여 자신의 비밀키 k_p를 암호화(= $E(SID, k_p)$)한 후 임시 인식자 ID_p와 함께 관리 서버에 전달한다. 여기서, 임시 인식자는 사용자가 사전에 등록한 보안 인식자 SID와 함께 관리서버에 등록한 임시 인식자를 의미한다.

$$\text{환자} \Rightarrow \text{관리서버} : E(SID, k_p), ID_p \quad (1)$$

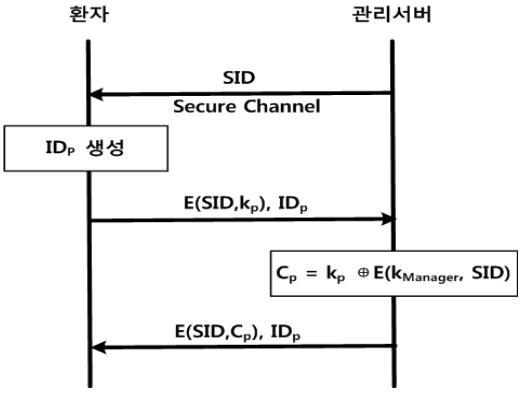

그림 7. 설정 단계
Fig. 7 Establishment Step

■ 2단계:

관리 서버는 환자로부터 전달받은 정보 중 임시 인식자 ID_p을 이용하여 데이터베이스에 저장되어 있는 환자의 보안 인식자를 검색한다. 만일 임시 인식자 ID_p와 일치하지 않으면 바로 종료한다. 관리 서버는 검색된 환자의 보안 인식자 SID를 통해 환자의 비밀키 k_p를 복호

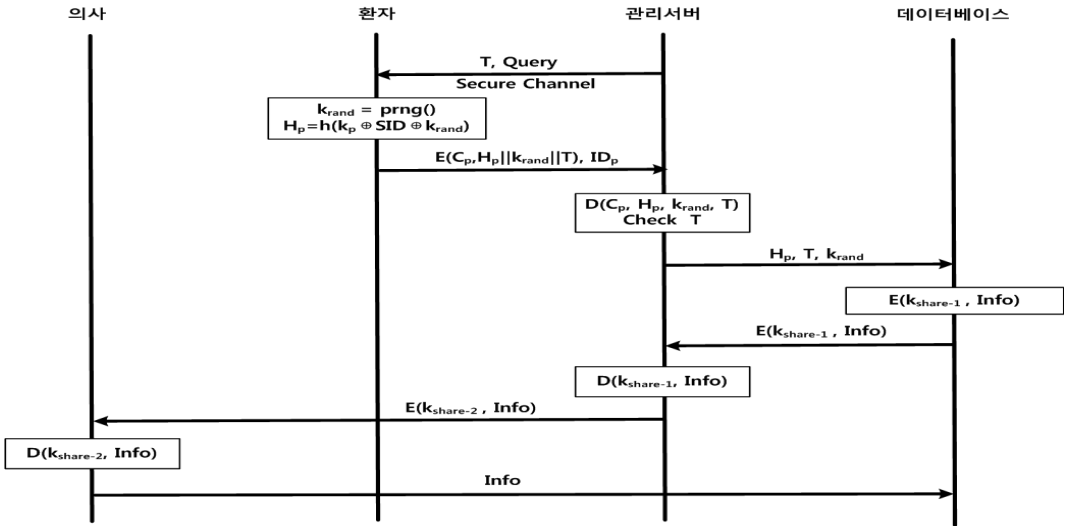

그림 8. 인증 단계
Fig. 8 Authentication Step

화하고 데이터베이스에 저장되어 있는 비밀키와 비교한다. 환자의 비밀키 무결성이 끝나면 서버는 자신의 생성한 비밀키 $k_{Manager}$를 이용하여 환자의 보안 인식자 SID를 $E(k_{Manager}, SID)$처럼 암호화한 후 환자의 비밀키 k_p와 XOR 연산을 수행한다. XOR 연산된 결과가 C_p로 대체된 후 C_p는 데이터베이스 테이블 내의 해당 환자 필드에 저장된다.

관리서버 : $C_p = k_p \oplus E(k_{Manager}, SID)$ (2)

■ 3 단계:

관리서버는 새로 생성된 환자의 비밀키 값 C_p를 사용자의 보안 인식자 SID로 암호화하여 환자에게 전달한다.

관리서버 $\Rightarrow$ 환자 : $E(SID, C_p), ID_p$ (3)

통신과정 중에 송·수신되는 메시지는 관리자가 선택적 평문 공격과 같은 공격으로 인해 악의적으로 타협될 수 있기 때문에 제안 프로토콜에서는 CRC(Cyclic Redundancy Check)과 같은 메커니즘을 적용하여 선택적 평문 공격을 예방하려고 한다. 또한 제안 프로토콜은 CRC 메커니즘을 적용하여 사용하였기 때문에 목적지까지 전송하려고 하는 원본 메시지에 추가적인 바이트를 피할 수 있다.

3.3.2. 인증 단계

인증단계는 환자의 인증 프로토콜의 구성과 동작과정을 보여주며, 환자 정보를 기반으로 u-헬스케어 서비스를 관리한다. 동작단계의 세부적인 동작 과정은 6단계로 동작한다.

■ 1단계 :

관리자는 타임스탬프 T를 생성하여 환자에게 쿼리 메시지 $Query$와 함께 전송한다. 타임스탬프 T는 하위계층의 환자와 상위계층의 병원사이의 시간 동기화를 위한 목적으로 사용된다.

관리서버 $\Rightarrow$ 환자 : T, Query (4)

■ 2단계 :

환자는 psedou 랜덤 넘버 함수 prng()로부터 생성한 임시 랜덤 값 k_{rand}을 관리 서버로부터 전달받은 타임스

탬프 T, 자신의 보안 인식자 SID, 비밀키 k_p을 H_p(=$h(k_p \oplus SID \oplus k_{rand} \oplus T)$)처럼 해쉬한다. 환자는 비밀키 값 C_p을 이용하여 $E(C_p, H_p \| k_{rand} \| T)$처럼 암호화한 후 관리서버에게 전달한다.

환자 ⇒ 관리서버 :

$$E(C_p, H_p \| k_{rand} \| T), ID_p \quad (5)$$

■ 3단계 :

관리서버는 수신한 메시지를 복호화한 후 자신이 정한 임계 시간내에 도착하였는지 타임스탬프 T를 검증한다. 만약 검증에 통과하지 못하면 인증과정을 종료하고 그렇지 않으면 환자가 병원 내/외에 있는지 확인하고 수신된 메시지를 데이터베이스에 저장한다.

관리서버 :

$$D(C_p, H_p, k_{rand}, T) \quad (6)$$

$$Check \quad T \quad (7)$$

■ 4단계 :

데이터베이스는 관리 서버로부터 전송받은 메시지 (H_p, T, k_{rand}) 중 H_p의 무결성을 검증하기 위해서 데이터베이스 내에 저장되어 있는 모든 정보 쌍 {SID,k_p}을 이용하여 관리 서버로부터 수신한 H_p값과 일치하는 {SID,k_p} 쌍을 검색한다. 만약 해당 환자 정보가 존재하지 않으면 오류 메시지를 관리서버에게 전달하고 그렇지 않으면 환자를 인증하고 환자에 대한 정보를 관리서버와 데이터베이스 사이에 공유한 공유키 $k_{share-1}$를 사용하여 관리서버에게 전달한다.

데이터베이스⇒관리서버 :

$$E(k_{share-1}, Info) \quad (8)$$

■ 5단계 :

관리서버는 정상적으로 환자가 인증되었을 경우 데이터베이스로부터 전달받은 환자의 개인정보를 복호화한다.

관리서버 :

$$D(k_{share-1}, Info) \quad (9)$$

■ 6단계 :

관리서버는 관리서버와 의사사이에 공유된 공유키 $k_{share-2}$로 의사에게 환자 정보를 전달한다.

관리서버 ⇒ 의사 :

$$E(k_{share-2}, Info) \quad (10)$$

의사 :

$$D(k_{share-2}, Info) \quad (11)$$

의사는 전달된 환자의 개인정보를 공유키 $k_{share-2}$을 이용하여 복호화한 후 의료 업무를 수행한다. 수행 완료된 업무 결과는 관리 서버를 통해 환자에게 전달되고 데이터베이스에 업무 결과를 저장한다.

의사⇒데이터베이스 :

$$Save \quad Info \quad (12)$$

3.3.3. 유지보수 단계

유지보수 단계에서는 환자의 개인정보를 암호화하기 위해 공유키를 사용하는데, 일정주기 동안공유키를 변경하지 않고 사용할 경우 악의적인 사용자로부터 보안 공격이 발생할 수 있다. 이런 보안 공격을 예방하기 위해서 환자 정보를 추가/삭제 시 임시 랜덤값을 정기적으로 갱신하는 방법을 이용하고 있다. 환자와 관리서버 사이에 공유된 공유키를 갱신하여 환자에게 전달함으로써 backward/forward secrecy를 예방할 수 있다.

① 악의적인 환자 처리: u-헬스케어 서비스를 제공받는 환자가 악의적이라고 판단되면 관리서버는 현재 악의적인 사용자가 사용하는 키를 변경함으로써 악의적인 환자를 u-헬스케어 환경으로부터 격리한다. 악의적인 환자를 격리하기 위해서는 관리서버가 보유하고 있는 데이터베이스 내 환자 목록으로부터 환자정보를 제거하고, u-헬스케어 서비스 접근에 필요한 키를 수정 및 삭제한다.

② 악의적인 환자 복구: 격리된 환자가 악의적인 상태로부터 회복되는 경우, 회복된 환자는 신규 인증 프로토콜 과정을 이용하여 u-헬스케어 서비스를 제공받을 수 있다. 환자가 동일한 공격으로 악의적으로 되는 것을 피하기 위해서는 환자가 u-헬스케어 서비스를 받기 전에 C_p와 공유 키가 다시 만들어져야 한다.

Ⅳ. 평가

이 절에서는 u-헬스케어에서 발생할 수 있는 가장 대표적인 공격유형으로 제안 프로토콜의 안전성을 평가한다.

4.1. 재전송 공격

u-헬스케어 환경에서는 환자와 병원사이에서 전송되는 환자 정보를 도청한 후 정당한 병원이나 환자로 위장할 수 있다. 제안 프로토콜은 병원과 환자사이에 매 세션 새로운 타임스탬프 T와 랜덤 값 k_{rand}을 생성하여 환자 인증을 수행한다. 제안 프로토콜에서는 게이트웨이 역할을 하는 관리 서버를 통해 환자를 인증하기 때문에 의사가 환자 정보를 판독하는 동안 악의적인 공격자가 방해하지 못하도록 한다. 이것은 중간 역할을 하는 관리 서버가 의사와 환자 사이에서 키 관리 역할을 수행하기 때문에 가능하다.

4.2. 스푸핑 공격

u-헬스케어에서 발생하기 쉬운 공격 중 하나가 스푸핑 공격이다. 이 공격은 병원과 환자사이에 공유된 비밀키 k_p을 얻음으로써 가능하다. 제안 프로토콜은 관리 서버와 환자사이에 전송되는 정보 $E(C_p, H_p, k_{rand}, T)$을 공격자가 얻더라도 암호화된 환자의 비밀키 C_p을 직접적으로 얻을 수 없어 스푸핑 공격을 수행할 수 없다. 만일 공격자가 환자의 비밀키 C_p을 얻더라도 사용자의 비밀키 k_p을 모르기 때문에 스푸핑 공격이 불가능하다.

4.3. 위치 트래킹 공격 및 위치 프라이버시

환자의 비밀키 k_p는 환자 자신만이 알고 있는 정보이며 주기적으로 다른 값으로 재생성되기 때문에 C_p(= $k_p \oplus E(k_{Manager}, SID)$) 또한 매 세션마다 새로 생성된다. 새로 생성된 C_p는 공격자가 현 세션에서 환자의 응답이 과거 세션에 도청한 응답과 동일한지 검증하는 것이 쉽지 않다. 제안 프로토콜은 공격자가 특정 환자를 식별할 수 없어 환자의 위치 트래킹 공격을 수행할 수 없어 환자의 프라이버시를 제공한다.

4.4. DB 정보 유출

관리 서버가 관리하는 데이터베이스 정보가 공격자에 의해 유출하였다고 가정하였을 경우 공격자는 암호화되어있지 않은 데이터베이스 파일을 쉽게 얻을 수 있다. 그러나 제안 프로토콜에서는 환자의 비밀키 k_p가 아닌 암호화된 C_p을 얻기 때문에 비밀키 k_p을 알지 못할 경우 복호화할 수 없다.

만일 공격자가 사용자의 비밀키 k_p을 얻더라도 C_p = $k_p \oplus E(k_{Manager}, SID)$로부터 $C_p \oplus k_p$을 계산하여 $E(k_{Manager}, SID)$을 얻을 수 있지만 서버 자신이 생성한 $k_{manager}$을 알 수 없어 환자의 비밀키에 대한 안전성을 보장할 수 있다. 제안 프로토콜은 합법적인 임의의 환자에 대한 데이터베이스 유출 공격에 대해서 안전한다.

4.5. 환자 익명성

관리서버는 타임스탬프 T을생성하여 환자에게 전송하면 환자는 수신한 타임스탬프 T와 환자 자신이 생성한 랜덤 값 k_{rand}과 H_p을 계산한다. 이때, H_p(=$h(k_p \| SID \| k_{rand} \| T)$)는 공격자가 복호화하려고 하더라도 환자 자신이 생성한 비밀 키 k_p, SID을 추측할 수 없기 때문에 환자의 익명성을 제공한다.

4.6. 보안 비교분석

[표 2]는 제안된 프로토콜이 [11]과 보안 평가 항목을 비교하여 개선된 점을 정리한 결과이다.

표 2. 안전성 분석 - [11]과 비교하여 개선된 측면
Table. 2 Compare Analysis of Security with [11]

항목	개선점
재전송 공격	[11]과 비교하여 제안 프로토콜은 중간 게이트웨이 역할을 하는 관리 서버가 키 관리 역할을 수행하도록 함으로써 의사가 환자 정보를 판독하는 동안 악의적인 공격을 예방
스푸핑 공격	[11]과 비교하여 제안 프로토콜은 병원과 환자 사이의 비밀키 k_p이외에 환자의 비밀키 C_P를 사용
위치 트래킹 공격	[11]과 비교하여 제안 프로토콜은 $C_p(= k_p \oplus E(k_{Manager}, SID))$를 매 세션마다 새로 생성하여 현 세션에서 환자의 응답이 과거 세션에 도청한 응답과 동일한지 검증이 불가능하도록 함
위치 프라이버시	[11]과 비교하여 제안 프로토콜은 환자가 보안 인식자 SID를 사용하여 공격자가 환자의 위치 트래킹 공격을 수행할 수 없어 환자의 프라이버시를 제공
DB 정보 유출	[11]과 비교하여 제안 프로토콜은 환자의 비밀키 k_p가 아닌 암호화된 C_p을 얻기 때문에 비밀키 k_p을 알지 못할 경우 복호화할 수 없도록 하여 DB 정보의 안전성 보장
환자 익명성	[11]과 비교하여 제안 프로토콜은 보안 인식자 SID를 사용하여 환자의 익명성 보장

4.7. 효율성 비교분석

[표 3]는 제안된 프로토콜과 [11]의 효율성을 비교분석한 결과이다. [표 3]에서 n은 데이터베이스에 저장된 환자의 최대수를 의미한다.

표 3. 효율성 비교분석
Table. 3 Compare Analysis of Efficiency

항목	[11]				제안 프로토콜			
	DB		관리자	환자	DB		관리자	환자
	유	무			유	무		
랜덤 값	0	0	0	1	0	0	0	1
타임스탬프	0	0	1	0	0	0	1	0
해쉬/ MAC 연산	n	$2n$	0	1	$\log_2 n$	$\log_2 n$	0	1
XOR 연산	0	0	0	0	0	0	0	0
통신 라운드 수	4							

[표 2]에서 [11]과 제안 프로토콜은 해쉬/MAC 연산 항목에서 성능 차이가 나타났으며 이 같은 결과는 데이터베이스에 접속할 때 사용되는 임시 인식자 ID_p를 통해 SID을 식별한 후 사용자와 관리자 사이에는 추가적인 해쉬/MAC 연산이 이루어지지 않고 (SID, k_p)쌍으로만 사용자와의 인증이 수행되기 때문이다. 특히 제안 프로토콜은 [11]과 같이 기존 RFID 인증 프로토콜의 태그 측에서 최대 n번의 해쉬 연산을 수행되는 연산 문제점을 1번만 수행하여 효율성을 향상시켰다.

V. 결론

본 논문에서는 환자가 소유하고 있는 휴대장치(PDAs나 휴대용 컴퓨터)를 제 3자가 불법적으로 악용하는 것을 예방하기 위한 RFID 기반의 보안 프로토콜을 제안하였다. 제안 프로토콜은 사전에 관리 서버에 등록된 사용자의 권한정보에 따라 환자의 개인정보에 접근하는 환자, 병원, 약국의 권한을 분리하여 최소한의 업무를 수행하도록 하였다. 특히, 게이트웨이 역할을 수행하는 관리 서버는 접근 허가가 승인된 환자 정보 이외에 허가받지 않은 정보에 제 3자가 쉽게 접근하지 못하도록 주기적으로 접근 허용 키를 생성하여 환자의 인증 및 관리의 효율성을 향상시켰다. 향후 연구에서는 제안된 메커니즘을 실제 환경에 적용할 계획이다.

참고문헌

[1] D. W. Kim, J. W. Han, and K. I. Chung, "Trend of Home Device Authentication/Authorization Technology", Weekly IT BRIEF, No. 1329, pp. 1-11, 2008.

[2] S.Y. Lee, K.B. Yim, K.J. Bae, Taeyoung Jeong, and Jong-Wook Han, "Counterplan of Ubiquitous Home Network Privacy based on Device Authentication and Authorization," Korea Institute of Information Security & Cryptology, Review of KIISC, 18(5), pp.125-131, 2008.

[3] IronKey, https://www.ironkey.com/

[4] P. J. Bakker et al. "Investing Secure USB sticks", Nov. 2007.

[5] J. H. Kim, J. W. Gi, and C. K. Kim, "A User Authentication Method between Domains Using Privilege Certificates", Korea Institute of Information Security&Cryptology, Journal of KIISC, 18(6A), pp. 75-83, 2008.
[6] J. S. Moon, D. G. Lee, I. Y. Lee, "Device Authentication/Authorization PRotocol for Home Network in Next Generation Security", Advances in Information Security and Assurance(ISA 2009), LNCS 5576, pp. 760-768, 2009.
[7] STEALTH MXP FAMILY MXI Security, http://www.mxisecurity.com/
[8] W. R. Jeon, Y. S. Choi, H. J. Jeong, F. Yang, D. H. Won and S. J. Kim, "Vulnerability Analysis on SanDisk Cruzer Micro Flash Memory", CISCW'07 Proceedings, Vol. 17, No. 2, Dec. 2007.
[9] W.J. Lee, and I.S. Jeon, "Attribute-base Authenticated Key Agreement Protocol over Home Network", Journal of Korea Institute of Information Security & Cryptology (KIISC), 18(5), pp.49-57, 2008
[10] "Device Certificate Profile for the Home Network", TTAS.KO-12.0052, 2007.
[11] E. J. Yoon and K. Y. Yoo, "Patient Authentication System for Mediacal Information Security using RFID", Korea Inforamtion and Communication Society, Vol. 35, No. 6, pp. 962-969, Jun. 2010.

저자소개

이봉근(Bong-Keun Rhee)

1982년 2월 : 숭실대학교 전자계산학과 학사
1985년 8월 : 숭실대학교 산업대학원 전자계산학과 석사
2000년 2월 : 충북대학교 대학원 전자계산학과 박사 수료
1986년 3월 ~ 현재 : 부산경상대학 소방안전계열 교수
※관심분야 : 네트워크 보안, 정보보안

정윤수(Yoon-Su Jeong)

1998. 청주대학교 전자계산학과 학사
2000. 충북대학교 대학원 전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사
2008.3 ~ 2009.8 충북대 및 한남대 시간강사
2009.9 ~ 2012.2 한남대학교 산업기술연구소 전임연구원
2012.3 ~ 현재 목원대학교 정보통신공학과 교수
※관심분야 : IPTV, 정보보호, 암호이론, Network Security, 유・무선통신보안

이상호(Sang-Ho Lee)

1976. 숭실대학교 전자계산학과 학사.
1981. 숭실대학교 전자계산학과 석사.
1989. 숭실대학교 전자계산학과 박사.
1981. 3. ~ 현재 충북대학교 소프트웨어학과 교수
※관심분야 : 네트워크보안, Protocol Engineering Network Management